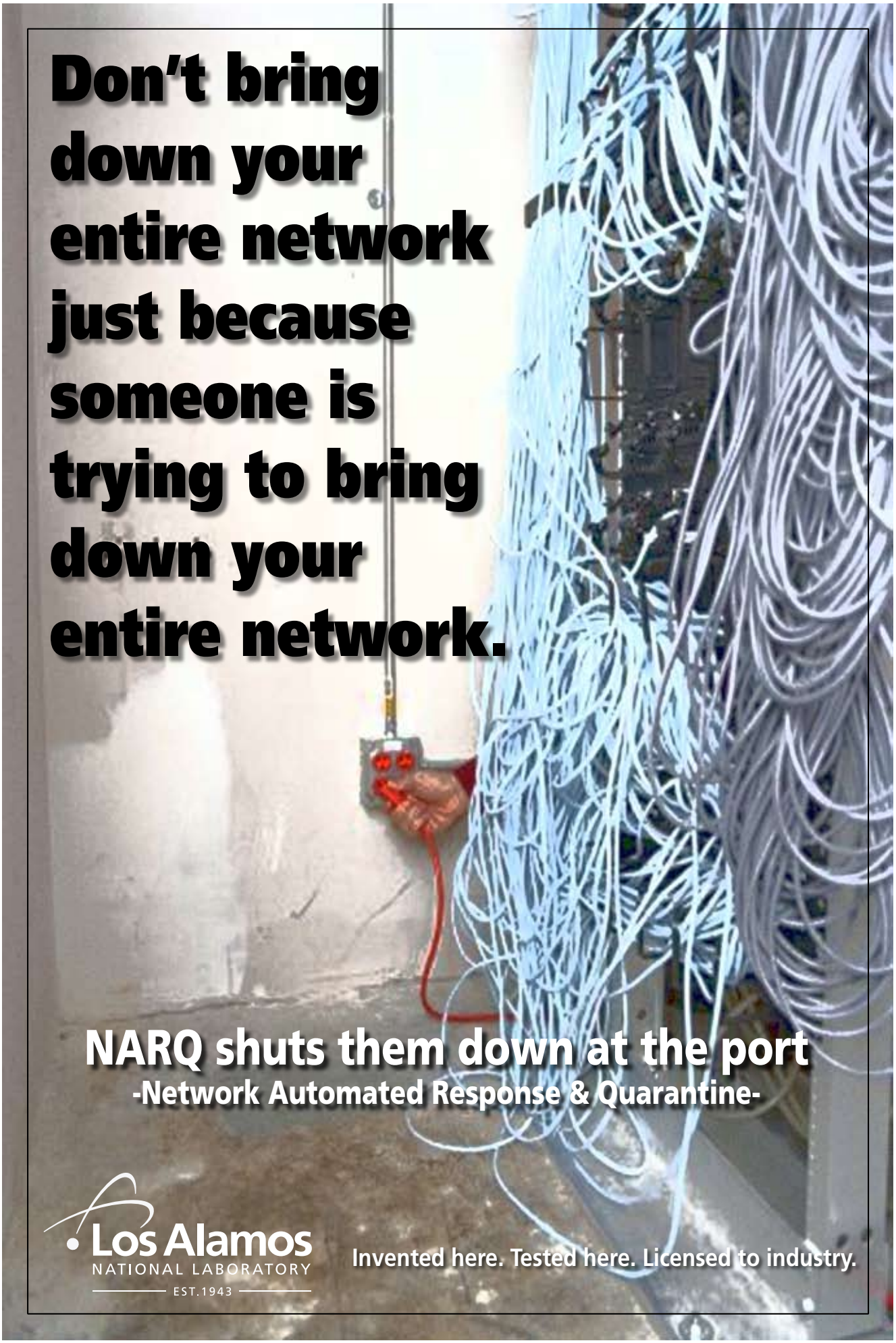
Don't bring down your entire network just because someone is trying to bring down your entire network.
NARQ shuts them down at the port
-Network Automated Response & Quarantine-
Los Alamos
NATIONAL LABORATORY
EST.1943
Invented here. Tested here. Licensed to industry.

LA-UR-05-5904

LOS ALAMOS NATIONAL LABORATORY

Technology Opportunity

Network Automated Response & Quarantine (NARQ™)

Applications

- Immediate response to detected invasive infections (worms)
- Quarantine removes infected computers and devices from the network at the port level
- Policy enforcement
- Vulnerability assessment and mitigation
- Network planning and optimization

Benefits

- Designed for robust and heterogeneous networks
- Instantaneous, automated reaction
- Low memory requirements
- Easy integration into existing detection packages
- Scriptable interface

Contacts

John R. Grizz Deal
Technology Transfer Division
Office: (505) 667-0878
Mobile: (505) 603-9096
grizz@lanl.gov

Brad Morie
Technology Transfer Division
Office: (505) 665-1578
morie@lanl.gov

Los Alamos NATIONAL LABORATORY ESTABLISHED 1943

The World's Greatest Science Protecting America

Summary

Since 1990, computer viruses and worms have cost companies worldwide nearly $2 billion in lost data, repair costs, and loss of productivity. Computer worms are programs that spread themselves from computer to computer over a network. Worms, unlike viruses, do not infect programs, diskettes, or files with macro capabilities, instead, they make copies of themselves and send these copies over the network to other targeted machines, ultimately bringing the entire enterprise down.

Enterprise networks are constantly changing, and becoming more and more complex, with hardware from a wide variety of disparate vendors—while IT staff is more burdened than ever due to financial constraints, evolving organizations, and ever more aggressive cyber terrorists.

Don't unplug it, use NARQ™!

Analogous to a biological infection, the only immediate and efficient manner in which to stop the spread of a worm is to stop it "at the port," or "at the wall jack;" at the edge of the network. The problem is not only identifying the affected device, but in determining physically where the device is located on the network, and then immediately reconfiguring the specific ports so as to shut down the infectious spread of the worm.

Los Alamos National Laboratory has developed a semi-automated and instantaneous layer-2 (Ethernet) network mapping and quarantine system. The Network Automated Response and Quarantine (NARQ™) software is designed to locate infected systems and then reconfigure ports so as to remove the infected devices from the network.

NARQ contains an instantly available graphical view of layer-2 switch interconnects and maps from the router to the desktop port. NARQ then applies the appropriate SNMP command to disconnect the affected devices from the enterprise network. A scriptable interface is provided for easy integration into existing applications. NARQ is several order of magnitudes faster than other solutions, was designed to work in heterogeneous, mission-critical networks, and on hardware from disparate vendors. NARQ was developed to protect the most sensitive network in the world.

Development Stage

NARQ has been in use for over a year at Los Alamos National Laboratory, reducing the response time to remove an infection from over three weeks to a few hours. Los Alamos has over 33 square miles of network infrastructure, VPN access, and over 10,000 computing devices. NARQ has been proven in the most robust and most sensitive enterprise in existence. The licensee will be provided inventor access, source code, and the commercial rights to the pending patent.

Intellectual Property Status

The instantaneous network mapping algorithm has been filed for U.S. patent protection.

Licensing Status

Available for co-exclusive licensing, on a royalty-bearing or one time fee basis. Los Alamos National Laboratory licenses select invented technologies to assist US companies in increasing their global competitive capabilities.

narq.lanl.gov